02

(19)日本国特許庁（ＪＰ） (12)公表特許公報（Ａ） (11)特許出願公表番号

特表平10－512074

(43)公表日 平成10年(1998)11月17日

(51)Int.Cl.*		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｚ
Ａ６３Ｆ	9/22		Ａ６３Ｆ	9/22	Ａ
Ｇ０６Ｆ	13/00	３５１	Ｇ０６Ｆ	13/00	３５１Ｅ
		３５５			３５５
	17/30		Ｇ０９Ｃ	1/00	６６０Ｃ

審査請求 未請求 予備審査請求 有 (全837頁) 最終頁に続く

(21)出願番号 特願平8－526318
(86) (22)出願日 平成8年(1996)２月13日
(85)翻訳文提出日 平成9年(1997)８月13日
(86)国際出願番号 ＰＣＴ／ＵＳ９６／０２３０３
(87)国際公開番号 ＷＯ９６／２７１５５
(87)国際公開日 平成8年(1996)９月６日
(31)優先権主張番号 ０８／３８８，１０７
(32)優先日 1995年２月13日
(33)優先権主張国 米国（ＵＳ）

(71)出願人 インタートラスト テクノロジーズ コーポレイション
アメリカ合衆国 カリフォルニア 94086－4708，サニーベール，オークメッド パークウェイ 460
(72)発明者 ジンター，カール エル．
アメリカ合衆国 メリーランド 20705，ベルツビル，43アールディー アベニュー 10404
(72)発明者 シェアー，ピクター エイチ．
アメリカ合衆国 メリーランド 20814，ベセスダ，バッテリー レーン 5203
(74)代理人 弁理士 山本 秀策

最終頁に続く

(54)【発明の名称】 安全な取引管理および電子権利保護のためのシステムおよび方法

(57)【要約】
本発明は、安全な取引管理および電子権利保護を有する電子商取引のシステムおよび方法を提供する。本発明に従って用いられるコンピュータなどの電子機器は、承認された様式でのみアクセスおよび使用されることを確実にし、情報の完全性、可用性、および／または秘匿性を維持する助けをする。このような電子機器と共に用いられる安全なサブシステムは、例えば、電子的に格納されたまたは広められた情報の使用を制御および／または計量もしくはモニタするために、処理と制御の安全なチェーンを実施し得る配布された仮想配布環境（ＶＤＥ）を提供する。このような仮想配布環境は、電子商取引および他の電子取扱または電子的に容易になった取扱において様々な参加者の権利を保護するために使用され得る。安全な配布されたおよび他の動作システム環境およびアーキテクチャは、例えば、各ノードで安全な保護された環境を確立し得る安全な半導体処理配置を使用する。これらの技術は、例えば、「電子ハイウェイ」を利用して用いられ得る終端間電子情報配布能力を支持するために使用され得る。

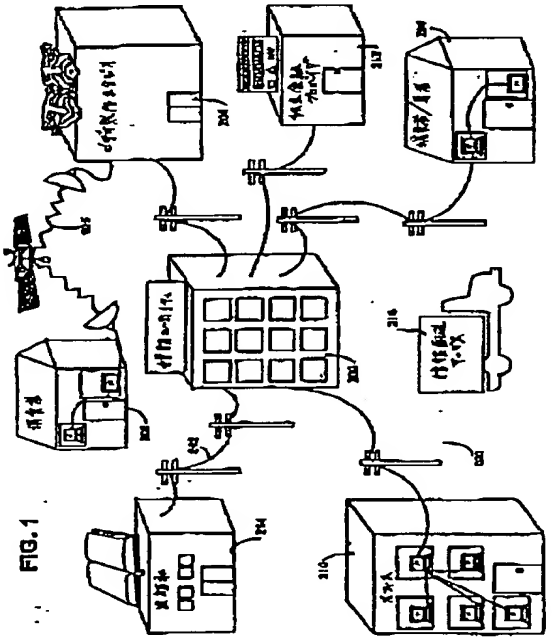

FIG. 1

化される。データブロック812は、やはりパーミッションレコード808内に提供される1つ以上のコンテンツ鍵を用いて暗号化され得る（情報あるいは管理的）コンテンツを有する。

2．移動オブジェクト

図19は、好適な実施形態によって提供される「移動オブジェクト」構造860の一例を示す。移動オブジェクトは、それらがVDEノードに到達したときにそれらのコンテンツの少なくとも一部の少なくとも部分的な使用を可能にするのに十分な情報を持っているオブジェクトである。

秘密ヘッダ804内にパーミッションレコード（PERC）808を有していることを除けば、移動オブジェクト構造860は、図18に示される静止オブジェクト構造850と同じである。移動オブジェクト構造860内にPERC 808を有していることによって、（メソッド1000および包含されるPERC 808に従って）あらゆるVDE電子機器／参加者600において移動オブジェクトを使用することが可能になる。

「移動」オブジェクトは、「チャネル外」配布を特にサポートし得るクラスのVDEオブジェクト300である。従って、移動オブジェクトは鍵ブロック810を有し、ある電子機器600から他の電子機器にトランスポート（transportable）可能である。移動オブジェクトには非常に限定された使用に関連する予算が付随している場合があり、これにより、ユーザは、（コンピュータプログラム、ゲーム、あるいはデータベース等の）コンテンツを全体的あるいは部分的に使用して、ライセンスを取得するのか、さらにライセンスするのか、あるいはオブジェクトコンテンツを購入するのかを判断することができる。あるいは、移動オブジェクトPERC 808は、例えば、

(a) 将来のライセンシングあるいは購入のために以前に購入した権利あるいは貸し方を反映するとともに、少なくとも1種類以上のオブジェクトコンテンツの使用を可能にする予算、および／または、

(b) オブジェクトコンテンツの使用を可能にするためにローカルVDEノードにおいて格納および管理された残っている(available)貸し方を採用する(およびこれを借方に記入し得る)予算、および／または、

(c) ローカルVDEノードへのレポート（さらに、任意に、情報交換所へのレポート）が要求される前の1つ以上の最大使用基準(maximum usage criteria)を反映するとともに、その後でリセットを行って、オリジナルの1つ以上の予算の中の1つ以上のさらなる使用および／または改変を可能にし得る予算、
を有する、あるいは、これを用いて予算レコードを参照することができる。

標準的なVDEオブジェクト300の場合のように、利用可能な予算を使いきった後にユーザがその移動オブジェクトを継続して使用しようとする場合、または、移動オブジェクト（あるいはそのコピー）が異なる電子機器に移動され、その新しい機器が、パーミッションレコード808によって要求される要件に対応する利用可能な貸し方予算を有していない場合、ユーザは、情報交換所サービスにコンタクトをとって付加的な予算を獲得するように要求される場合がある。

例えば、移動オブジェクトPERC 808は、要求される予算VDE1200あるいは利用可能であると認められるおよび／または利用可能になることが予想される予算オプションに対するリファレンスを有し得る。予算VDEは、消費者のVISA、MC、AMEX、またはオブジェクト独立型であり、且つ特定のあるいは複数クラスの移動オブジェクトコンテンツの使用に適用可能な他の「一般(generic)」予算（例えば、Blockbuster Videoレンタルであり得るあるクラスの移動オブジェクトからのあらゆる映画オブジェクト(movie object)）を参照し得る。予算VDE自身は、それと共に使用され得る1つ以上のクラスのオブジェクトを要求し得、あるオブジェクトは特定の1つ以上の一般予算を特に参照し得る。このような場合、典型的に、VDEプロバイダは、正しい参照を可能にするとともに課金処理および結果的な支払を可能にするような方法で情報を提供する。

機器が、一般に若しくは特定の1つ以上のユーザあるいはユーザクラスに対して、正しい予算あるいは予算の種類（例えば、VISA予算等の情報交換所から利用可能な十分な貸し方）を有する限り、または、その移動オブジェクト自身が十分な予算割当額(budget allowance)若しくは適切な承認を有する限り、移動オブジェクトは受信VDEノード電子機器600において使用できる（例えば、その移動オブジェクトが特定の1つ以上のインストレーション若しくはインストレーションク

ラスあるいはユーザ若しくはユーザクラスに対して使用可能であるという規定(stipulation)。但し、クラスは、安全なデータベース610に格納され予め定義されたクラス識別名(identifiers)によって表されるインストレーション若しくはユーザの特定の部分集合に対応)。移動オブジェクトを受け取った後、ユーザ(および/またはインストレーション)が適切な予算および/または承認を有していない場合、ユーザは、電子機器600によって(その移動オブジェクト内に格納された情報を用いて)、どの1つ以上のパーティに対してユーザがコンタクトをとり得るのかを知らされる。そのパーティは、(そこからユーザが所望のコンタクトを選択する)移動オブジェクトの情報交換所プロバイダの択一的なリストを構成し得る。

上記のように、移動オブジェクトは、「チャネル外に」オブジェクト300を配布することを可能にする。つまり、オブジェクトは、不許可のあるいは明示的には

許可されていない個人から別の個人に配布され得る。「チャネル外」は、例えばユーザがあるオブジェクトを別の個人に直接的に再配布することを可能にする配布経路(path of distribution)を含む。例えば、オブジェクトプロバイダは、ユーザがあるオブジェクトのコピーをそのユーザの友人若しくは同僚に(例えば、記憶媒体の物理的な配送、あるいは、コンピュータネットワーク上での配送によって)再配布することを可能にして、これにより、友人若しくは同僚がそのオブジェクトを使用するために要求される何らかの特定の基準を満たした場合にその友人若しくは同僚に使用を許可することが可能である。

例えば、ソフトウェアプログラムが移動オブジェクトとして配布された場合、そのプログラムのユーザが、そのソフトウェアあるいはそのソフトウェアの使用可能なコピーを友人に供給したいと願っている場合、通常は自由にそうすることができる。移動オブジェクトには、大きな商業的価値が秘められている。なぜなら、有用なコンテンツは主にユーザおよび電子掲示板によって配布され得、「オリジナル」コンテンツプロバイダおよび/または情報交換所への登録の他には配布オーバーヘッドがほとんどあるいは全く必要でないからである。

「チャネル外」配布は、プロバイダが、使用に対する支払を受け取ることおよび／または再配布されたオブジェクトの少なくともある程度の制御を別の方法で維持することをも可能にし得る。このような特定の基準は、例えば、その使用のために十分に利用可能な貸し方のあるクレジットカード等の承認されたサードパーティ金融関係のユーザVDEノードにおける登録された存在を含み得る。

従って、ユーザがVDEノードを持っていた場合、もしユーザが、ユーザのVDEノード上で利用可能な（また、必要な場合、ユーザに割り当てられた）適切な利用可能な予算を持っていたならば、および／または、もしユーザまたはユーザのVDEノードが、特別に承認されたグループのユーザ若しくはインストレーションに属していたならば、および／または、もし移動オブジェクトがそれ自身の予算を持っていたならば、そのユーザはその移動オブジェクトを使用することができるかもしれない。

移動オブジェクトのコンテンツは暗号化されており、そのオブジェクトに用いられている移動オブジェクト秘密ヘッダ鍵が破損していない限り、移動オブジェクトのコンテンツは、承認された状況下でのみ使用できる。これは、例えば、パーミッションおよび／または予算情報に比べた場合、移動オブジェクトの比較的容易なタスクであり得る。なぜなら、多数のオブジェクトが同一の鍵を共有しており、分析すべきよりたくさんの暗号文情報と暗号解析を行うより強い動機の両方を暗号解析者に与え得るからである。

「移動オブジェクト」の場合、コンテンツの所有者は、そのコンテンツがカプセル化されているオブジェクト300内に含まれている鍵ブロック810の一部あるいはその全てとともに情報を配布し得る。配布されるオブジェクト300内に鍵を置けば、秘密ヘッダの保護に用いられている暗号化アルゴリズムを破るあるいは暗号解析することによって（例えば、ヘッダの暗号化の鍵を決定することによって）セキュリティメカニズムを突破しようとする試みに曝される危険性が増大する。セキュリティの突破は通常、相当な技術と時間を要するが、もし突破された場合、そのアルゴリズムおよび鍵が公開されて、これと同一の鍵およびアルゴリズムによってプロテクトされているオブジェクトを持っている多数の個人がプロテ

クトされた情報を不正使用できるようになる。結果的に、配布されるオブジェクト300内に鍵を置くことは、「時間に左右される」（特定の期間経過後には値が減少している）あるいはその値が幾分制限されるコンテンツ、または、鍵をオブジェクト内に置く商業的価値（例えば、エンドユーザにとっての便利さ、遠距離通信あるいは鍵および／またはパーミッション情報を配送する他の手段および／または「チャネル外」に出ていくオブジェクトのサポートに対する能力を排除する比較的低いコスト）が、高度なハッカーに対する被攻撃性のコストを上回る場合に限定され得る。他の箇所で述べられているように、旋回技術を採用して移動オブジェクト内に「真性(true)」鍵を格納しないようにすることによって、鍵のセキュリティを高めることができるが、ほとんどの場合、サイトIDおよび／または時刻ではなくて、VDE管理者によってほとんどあるいは全てのVDEノードに入力として提供される共有のシークレット(shared secret)を用いることによってオブジェクトをこれらの値から独立した状態に維持する。

図19に示し、先に述べたように、移動オブジェクトは、好ましくは少なくとも何らかの予算（一般的な場合、一方、他方、あるいは両方）を提供するパーミッションレコード808を有する。上記のように、パーミッションレコード808は、重要な鍵情報を格納している鍵ブロックを有し得る。PERC 808は、有価数量(valuable quantities)／値(values)を有する可能性のある予算を持っているか、あるいはこれを参照し得る。このような予算は、移動オブジェクト自身の中に格納されるか、あるいは、別々に配送されて高度安全通信鍵および管理的オブジェクト鍵および管理データベース技術によって保護され得る。

移動オブジェクトに含まれるメソッド1000は、典型的に、オブジェクト内のパーミッションレコード808（例えば、REGISTERメソッド）を用いてそのオブジェクトを「自己登録」するためのインストレーションプロシージャを含む。これは、時間制限値を有するオブジェクトと、エンドユーザが料金を請求されないあるいは所定料金しか請求されないオブジェクト（あるいはプロパティ）（例えば、公開情報に実際にアクセスしたエンドユーザの数に基づいて広告主および／または情報発行者が料金請求されるオブジェクト）と、広く利用可能な予算を要求す

るとともにチャネル外配布から特に恩恵を受け得るオブジェクト（例えば、クレジットカードから派生する、映画、ソフトウェアプログラム、ゲーム等のプロパティを有するオブジェクトのための予算）とに特に有用であり得る。このような移動オブジェクトは、予算UDEを含んであるいは含まずに供給され得る。

移動オブジェクトの１つの使用方法であるソフトウェアの発行においては、顧客になる可能性のある者が、ライセンス料金を支払う前あるいは初期試用料金以上の料金を支払う前に、そのソフトウェアをデモンストレーションモードで使用する、あるいは可能であれば限られた期間内において完全なプログラム機能を使用することを、包含されるパーミッションレコードによって許可し得る。例えば、時間ベースの課金方法および小さな時間予算が予備インストールされた予算レコードを用いて、短い期間の間そのプログラムを完全に使用することを許可する。オブジェクトコンテンツの不正使用を回避するために様々な制御メソッドを用いることが可能である。例えば、移動オブジェクトの最小登録期間をある適切な長い期間（例えば、１ヶ月、６ヶ月あるいは１年間）に設定することによって、ユーザが同一の移動オブジェクト内の予算レコードを繰り返し使用することを防ぐことができる。

移動オブジェクトの使用を制御するもう１つの方法は、その移動オブジェクト内に組み込まれたパーミッションレコードに経時変化鍵を含めることである。これは、移動オブジェクトが、再登録を行うことなく特定日以降に使用されないようにするためのもので、一般に移動オブジェクトに有用であり、一斉通信、ネットワークあるいは（１方向および２方向ケーブルの両方を含む）遠距離通信によって電子的に配布される移動オブジェクトに特に有用である。なぜなら、このような移動オブジェクト経時変化鍵の配送の日付および時刻は、ユーザがそのオブジェクトの所有権を得た時刻に正確に対応するように設定できるからである。

移動オブジェクトを使用して、ある電子機器600から別の電子機器への「移動」を助長することも可能である。ユーザは、１つ以上のパーミッションレコード808が組み込まれた移動オブジェクトを、例えばデスクトップコンピュータから同じユーザのノートブックコンピュータへと移動させることができる。移動オブ

ジェクトがそのユーザをオブジェクト自身の中に登録して、その後はそのユーザしか使用できないようにすることが可能である。移動オブジェクトは、基本配布予算レコード用に1つ、および、登録ユーザの「アクティブ」配布予算レコード用のもう1つといった別々の予算情報を維持し得る。このようにすれば、オブジェクトをコピーしてユーザになり得る別の者に引き渡して、その後は、これを、そのユーザのためのポータブルオブジェクトとすることが可能である。

移動オブジェクトが他のオブジェクトを有するコンテナ内に入っている場合もある。例えば、移動オブジェクトコンテナは、コンテンツオブジェクトをエンドユーザオブジェクトレジストリ内に登録するため、および/または、パーミッションおよび/または他のセキュリティ機能を施行するためのメカニズムを提供するための、1つ以上のコンテンツオブジェクトおよび1つ以上の管理的オブジェクトを有し得る。包含された管理的オブジェクトを用いて必要なパーミッションレコードおよび/または予算情報をエンドユーザの電子機器内に設置(install)することが可能である。

コンテンツオブジェクト

図20は、VDEコンテンツオブジェクト構造880の一例を示す。コンテンツオブジェクト880は、概して、情報コンテンツを有するあるいは提供する。この「コンテンツ」は、任意の種類の電子情報であり得る。例えば、コンテンツには、コンピュータソフトウェア、映画、本、音楽、情報データベース、マルチメディア情報、バーチャルリアリティ情報、機械命令、コンピュータデータファイル、通信メッセージおよび/または信号、ならびに、少なくともその一部が1つ以上の電子機器によって使用あるいは操作される他の情報が含まれる。また、銀行間での取引、電子購入通信、ならびに、電子的に署名された契約書および他の法的な書類の送信、監査および秘密保護された商業記録等の電子商取引および通信について、これらの認証、制御および/または監査用にVDE 100を構成することも可能である。これらの取引に用いられる情報もまた、「コンテンツ」と呼ぶことができる。先に述べたように、このコンテンツは物理的にオブジェクトコンテナ内に格納される必要はなく、異なる時刻に別々に提供され得る(例えば、ケーブルに

【図19】

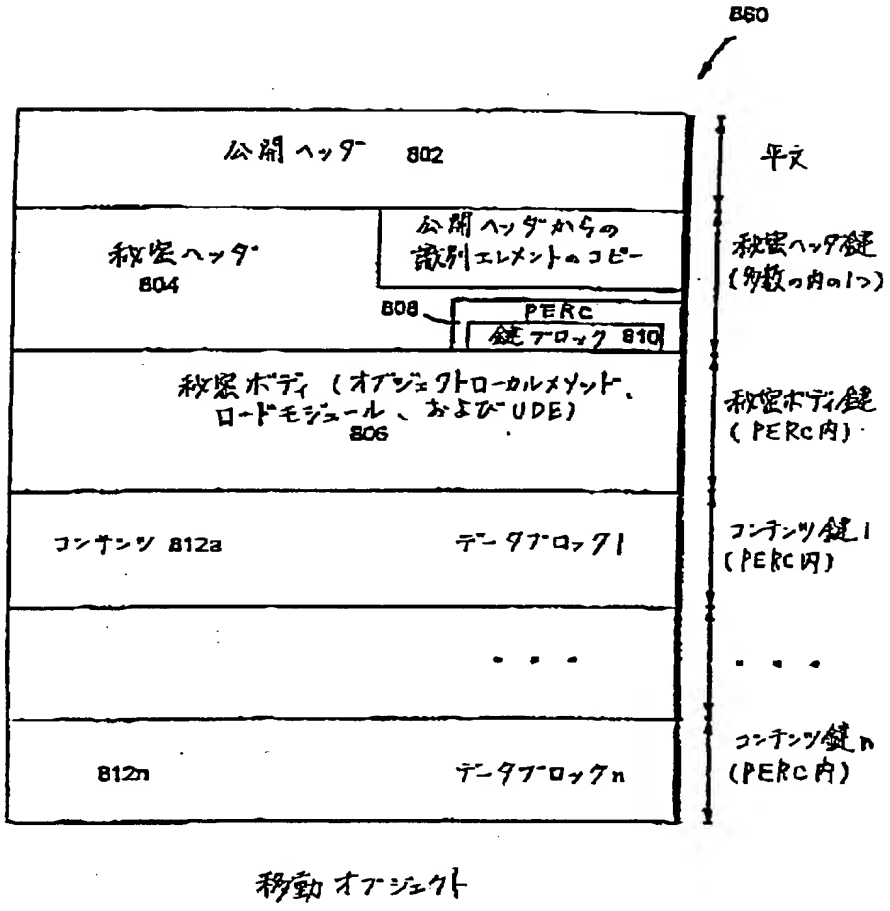
850
公開ヘッダ 802
平文
秘密ヘッダ
804
公開ヘッダからの
識別エレメントのコピー
秘密ヘッダ鍵
(多数の内の1つ)
808
PERC
鍵ブロック 810
秘密ボディ(オブジェクトローカルメソッド、
ロードモジュール、およびUDE)
806
秘密ボディ鍵
(PERC内)
コンテンツ 812a
データブロック1
コンテンツ鍵1
(PERC内)
812n
データブロックn
コンテンツ鍵n
(PERC内)
移動オブジェクト

FIG. 19

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.